UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

MISTY MEIER, on behalf of her minor child G.C-M., and JANE DOE, individually and on behalf of all others similarly situated, Plaintiffs, v. NETGAIN TECHNOLOGY, LLC, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Misty Meier, on behalf of her minor child, G.C-M., and Jane Doe, individually and on behalf of all others similarly situated, by and through their attorneys, bring this class action against Netgain Technology, LLC ("Netgain" or "Defendant").

INTRODUCTION AND NATURE OF ACTION

1. Plaintiffs bring this class action against Defendant Netgain Technology, LLC for its failure to secure and safeguard the confidential, personally identifiable information of hundreds of thousands of consumers. Although the information stolen varied by individual, the categories included names, account numbers, Social Security numbers, driver's license numbers, bank account numbers, and dates of birth ("PII"), as well as personal health information such as medical record numbers, health insurance policy and identification

numbers, clinical notes, referral requests, laboratory reports, decision not to vaccinate forms, immunization information, medical disclosure logs, in addition to other medical or health related information ("PHI"), hereinafter ("PII/PHI").

2. Netgain provides cloud-enabled IT solutions and managed services to various types of business entities including healthcare providers and accounting companies.

3. Netgain has provided IT solutions for organizations for almost 20 years, and has offices and data centers in Chicago, Minneapolis, San Diego, and Phoenix. With approximately 130 employees across its locations, Netgain generates $32.35 million dollars in sales.[1]

4. Indeed, Netgain offers cybersecurity solutions, yet failed to secure its own systems from cybercriminals.

5. In late September 2020, and due to Netgain's inadequate data security and failure to comply with federal and state data privacy standards, an unauthorized third party used compromised credentials to gain access to Netgain's digital environment. Thereafter, the unauthorized third party gained access to, and then exfiltrated, the files and records of various businesses that are customers of Netgain, including Neighborhood Healthcare, Health Center

[1] https://www.dnb.com/business-directory/company-profiles.netgain_technology_llc.52f33163cb3c315c73f15169f269e977.html

Partners of Southern California, Woodcreek Provider Services, LLC, Apple Valley Clinic/Allina Health, Ramsey County, Sandhills Medical Foundation, and Crystal Practice Management. In late September 2020, an unidentified third party launched a ransomware attack against Netgain using the data exfiltrated. Netgain claims to have paid an undisclosed amount to the cybercriminal in exchange for assurances that the criminal will delete all copies of the data obtained and that it would not publish, sell, or otherwise disclose the data. This series of events is referred to herein as the "Data Breach."

6. Due to Netgain's negligence and inadequate data security, Plaintiffs and Class members have suffered irreparable harm and are subject to an increased risk of identity theft. Plaintiffs' and Class members' PII/PHI have been compromised and they must now undertake additional security measures to minimize the risk of identity theft.

JURISDICTION AND VENUE

7. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members.

8. This Court has jurisdiction over Defendant because Netgain Technology, LLC maintains its principal place of business in Minnesota, regularly

conducts business in Minnesota, and has sufficient minimum contacts in Minnesota. Defendant intentionally availed itself of this jurisdiction by marketing and selling products and services from Minnesota to many businesses nationwide.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant Netgain Technology, LLC's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

PARTIES

10. Plaintiff Misty Meier is a resident of Riverside, California, who brings this lawsuit on behalf of her minor child, G.C-M., also a resident of Riverside, California. Meier and G.C-M. received a notice, dated April 8, 2021, that G.C-M.'s PII/PHI may have been stolen from Neighborhood Healthcare because its IT service provider, Netgain Technology, LLC experienced the Data Breach.

11. Plaintiff Jane Doe is a resident of San Diego County, California. She received a notice, dated May 7, 2021, that her PII/PHI may have been stolen from Health Center Partners of Southern California because its IT service provider, Netgain Technology, LLC experienced the Data Breach.

12. Defendant Netgain Technology, LLC is an American cloud-based IT services provider based in St. Cloud, Minnesota and incorporated in Delaware.

FACTUAL BACKGROUND

13. Netgain was founded in 2000 under the premise "that there had to be a better way to implement, manage and support IT."[2] As a provider of new and innovative IT services and solutions, Netgain proclaims to have revolutionized the industry for support and help desk experiences for organizations across various industries. By 2004, Netgain found its niche in specialized healthcare service and support, only a few years after its inception. As a provider of cybersecurity solutions, among other IT services, Netgain has both the duty and the expertise to safeguard the data of the organizations receiving its services. Plaintiffs and Class members had a reasonable expectation that Netgain would safely and securely store their PII and especially their PHI from digital theft and misuse.

14. As detailed more fully below, Netgain failed to safely and securely store the PII and PHI entrusted to it and failed to prevent it from being compromised during the Data Breach.

A. The Data Breach

15. Netgain claims to be the industry standard for secure and scalable IT as a Service for accounting and healthcare businesses.[3] As such, Netgain is well

[2] https://netgaincloud.com/about-us/history/ (last visited April 28, 2021).
[3] https://netgaincloud.com/about-us/

aware the accounting and healthcare industries process the most valuable data for cybercriminals.

16. In fact, Netgain touts its data security measures are like "Housing user data within the granite confines of a former Federal Building" which "ensures a level of structural stability that our clients trust."[4] Yet, while its customers reasonably believed their data was safe within Netgain's confines, between September 2020 and November 2020 Netgain's guard was down and cyber criminals infiltrated Netgain's walls.

17. In late September through December 2020, Netgain was subjected to a ransomware attack that targeted Netgain's domain controllers, which manage networks of thousands of servers. Included in the ransomware attack was the PII/PHI provided to Netgain it by certain of its clients. Shortly thereafter, Netgain began emailing its clients that it was going to shut down data centers in an effort to isolate the ransomware and rebuild the affected systems.

18. In January, Netgain began notifying its clients their information may have been compromised in the ransomware attack.

19. For example, in a Notification Letter to Woodcreek Provider Services, LLC, Netgain reported "a security incident that involved unauthorized access to

---

[4] *Id.*

portions of the Netgain environment which Netgain had discovered in late November 2020 but may have occurred as early as September 2020." The cyber criminals launched a ransomware attack, encrypting a subset of the PII/PHI of Netgain's clients and internal systems. In response, Netgain reported it took measures to contain the threat, including disabling external and internal network pathways and taking client services offline.[5]

20. Various notices have indicated the stolen PII/PHI included full names, dates of birth, bank account and routing numbers, Social Security numbers, driver's license numbers, medical records, health insurance policy numbers, and employee health information. Plaintiff Meier's notice on behalf of G.C-M. indicated the "information involved may have included some of the following: your name, date of birth, address, and information about the care you received from Neighborhood Healthcare such as insurance coverage information, physician you saw and treatment codes." Plaintiff Doe's notice indicated the "information involved…may include the following: name, date of birth, Social Security number, diagnosis/treatment information, provider name, medical record number, and treatment cost information."

[5] https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/WoodcreekProviderServicesLLC.2021-02-17.pdf

21. However, notice Netgain provided to some of its clients, including Plaintiffs' health care provider, Health Center Partners of Southern California ("HCP"), was unreasonably delayed. Plaintiffs were not informed of the Data Breach until April 12, 2021 and May 7, 2021, although the breach "may have occurred as early as September 2020."[6] Plaintiffs did not know to take action to secure their PII/PHI and mitigate any associated risks or harm until over six months after the breach occurred.

1. Data Breaches Lead to Identity Theft and Cognizable Injuries.

22. The personal, health, and financial information of consumers, such as Plaintiffs and Class members, is valuable and has been commoditized in recent years.

23. The ramifications of Defendant's failure to keep Plaintiffs' and Class members' PII and PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

24. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

---

[6] *Id.*

25. Stolen PII/PHI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

26. Once PII/PHI is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the original victim.

27. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

28. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiffs and Class members that their PII/PHI had been stolen.

29. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

30. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII/PHI to others who do the same.

31. Moreover, in light of the current COVID-19 pandemic, Plaintiffs' sensitive information could be used to fraudulently obtain any emergency stimulus or relief payments or any additional forms monetary compensation, unemployment and/or enhanced unemployment benefits.

32. Victims of identity theft often suffer indirect financial costs as well, including the costs incurred due to litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit.

33. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII/PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

34. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII/PHI. To protect

themselves, Plaintiffs and Class members (and the business entities whose information was breached) will need to be remain vigilant against unauthorized data use for years or even decades to come.

35. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point: Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.

36. Recognizing the high value consumers place on their PII/PHI, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share and who ultimately receives the information. And, by making the transaction transparent, consumers—not criminals—will be compensated.[7]

---

[7] *See* Steve Lohr, You Want My Personal Data? Reward Me for It, The New York Times, *available at* http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited April 28, 2021).

37. Consumers place a high value on their PII and a greater value on their PHI, in addition to the privacy of same. Research shows how much consumers value their data privacy, and the amount is considerable.

38. By virtue of the Data Breach here and unauthorized release and disclosure of the PII/PHI of Plaintiffs and the Class, Defendant has deprived Plaintiffs and the Class of the substantial value of their PII/PHI, to which they are entitled. As previously alleged, Defendant failed to provide reasonable and adequate data security, pursuant to and in compliance with industry standards and applicable law.

39. As a cybersecurity expert, Defendant is aware of the potential harm caused by this data theft, and even offers cyber security best practices tips.[8] In fact, in a March 24, 2021 blog entitled "What we learned as a ransomware victim – so you don't become one," Netgain writer Patrick Williamson admits Netgain identified "additional opportunities to strengthen our security posture in a continuous journey with an ongoing commitment to ensure this remains top-of-mind."[9] Netgain, as a company profiting from its cybersecurity services,

---

[8] *See* Kris Tufto, How Costly is a Data Breach, *available at* https://netgaincloud.com/blog/how-costly-is-a-data-breach/ (last visited April 28, 2021).

9 *See* What we learned as a ransomware victim – so you don't become one, *available at* https://netgaincloud.com/blog/what-we-learned-as-a-ransomware-victim-so-you-dont-become-one/ (last visited April 28, 2021).

understands better than most how important data security is and the ongoing nature of maintaining the latest technology and protocols for cyber security.

40. According to the Federal Trade Commission ("FTC"), unauthorized PII/PHI disclosures wreak havoc on consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[10]

41. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen.

42. As a result, victims suffer immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

43. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When such sensitive information is stolen, accounts become less secure and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

---

[10] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), *available at* http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited April 28, 2021).

44. As a direct and proximate result of Defendant's wrongful actions or omissions here, resulting in the Data Breach and the unauthorized release and disclosure of Plaintiffs' and other Class members' PII/PHI, Plaintiffs and the other Class members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) the untimely and inadequate notification of the Data Breach, (ii) the resulting immediate increased risk of future ascertainable losses, economic damages and other actual injury and harm, (iii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; and (iv) out-of-pocket expenses for securing identity theft protection and other similar necessary services.

45. Plaintiff Meier's minor child G.C-M. received treatment at one of Neighborhood Healthcare's locations which used Defendant as a third-party hosting provider.

46. According to the Notice, Plaintiff `C-M.'s PHI, stored on Defendant's system was determined to be impacted.

47. Defendant offered free credit monitoring which does nothing to protect Plaintiff Meier's minor child G.C-M. because he must have established credit to enroll. As a minor, he does not have established credit.

48. According to Robert P. Chappell Jr., a law enforcement professional, a child's information can be stolen at birth and used until the child turns eighteen years old before the child realizes they've been victimized.[11]

49. The risk to Plaintiff Meier's child G.C-M., as a minor, is substantial given his lack of established credit because his information can be used to create a "clean identity slate."

50. Plaintiff Doe received treatment at one of Health Center Partners of Southern California's member organizations which used Defendant as a third-party hosting provider.

51. According to the Notice, Plaintiff Doe's PII/PHI, stored on Defendant's system, was determined to be impacted.

52. Since receiving the Notice dated May 7, 2021, Plaintiff Doe has monitored her credit using Credit Karma.

CLASS DEFINITION AND ALLEGATIONS

53. Plaintiffs bring this class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following classes:

[11] https://www.parents.com/kids/safety/tips/what-is-child-identity-theft/ (last accessed on May 10, 2021)

The Nationwide Class:

> All persons residing in the United States who had their PII and/or PHI hosted by Netgain compromised as a result of the Data Breach.

The California Subclass:

> All persons residing in the State of California who had their PII and/or PHI hosted by Netgain compromised as a result of the Data Breach.

Collectively, the Nationwide Class and the California Subclass with be referred to as "the Class" unless there is need to differentiate them. Excluded from the Class are: (i) Defendant and its officers, directors, affiliates, parents, and subsidiaries (ii) the Judge presiding over this action, and (iii) any other person or entity found by a court of competent jurisdiction to be guilty of initiating, causing, aiding or abetting the criminal activity occurrence of the Data Breaches or who pleads nolo contendere to any such charge.

54. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

55. The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiffs are informed and believe that the proposed Class includes hundreds of thousands of Defendant's customers who have been damaged by Defendant's conduct as alleged herein. The precise number of Class

members is unknown to Plaintiffs but may be ascertained from Defendant's records.

56. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members. These common legal and factual questions include, but are not limited to, the following:

a. whether Defendant engaged in the wrongful conduct alleged herein;

b. whether the alleged conduct constitutes violations of the laws asserted;

c. whether Defendant owed Plaintiffs and the other Class members a duty to adequately protect their PII/PHI;

d. whether Defendant breached its duty to protect the personal and financial data of Plaintiffs and the other Class members;

e. whether Defendant knew or should have known about the inadequacies of their data protection, storage, and security;

f. whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiffs' and the other Class members' PII/PHI from unauthorized theft, release, or disclosure;

g. whether the proper data security measures, policies, procedures and protocols were in place and operational within Defendant's offices

and computer systems to safeguard and protect Plaintiffs' and the other Class members' PII/PHI from unauthorized theft, release or disclosure;

h. whether Defendant breached its promise to keep Plaintiffs' and the Class members' PII/PHI safe and to follow federal data security protocols;

i. whether Defendant violated § 1798.150 of the California Consumer Privacy Act by failing to prevent Plaintiffs' and Class members' PII/PHI from unauthorized access and exfiltration, theft, or disclosure, as a result of Defendant's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information;

j. whether Defendant's misconduct identified herein amounts to a violation of Cal. Bus. & Prof. Code § 17200, et seq.;

k. whether Defendant's conduct was the proximate cause of Plaintiffs' and the other Class members' injuries;

l. whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

m. whether Plaintiffs and the other Class members suffered ascertainable and cognizable injuries as a result of Defendant's conduct;

n. whether Plaintiffs and the other Class members are entitled to recover actual damages and/or statutory damages; and

o. whether Plaintiffs and the other Class members are entitled to other appropriate remedies, including injunctive relief.

57. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiffs on behalf of themselves and the other Class members. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

58. Plaintiffs' claims are typical of the claims of the members of the Class. All Class members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class members in a similar manner.

59. Plaintiffs will fairly and adequately protect the interests of the members of the Class, have retained counsel experienced in complex consumer class action litigation, and intend to prosecute this action vigorously. Plaintiffs have no adverse or antagonistic interests to those of the Class.

60. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their

claims against Defendant. It would thus be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done to them. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts and would also increase the delay and expense to all parties and the courts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

61. Plaintiffs incorporate by reference all previous allegations as though fully set forth herein.

62. Upon gaining access to the PII/PHI of Plaintiffs and members of the Class, Defendant owed to Plaintiffs and the Class a duty of reasonable care in handling and using this information and securing and protecting the information from being stolen, accessed, and misused by unauthorized parties. Pursuant to this duty, Defendant was required to design, maintain, and test their security systems to ensure that these systems were reasonably secure and capable of protecting the PII/PHI of Plaintiffs and the Class. Defendant further owed to Plaintiffs and the Class a duty to implement systems and procedures that would detect a breach of

their security systems in a timely manner and to timely act upon security alerts from such systems.

63. Defendant owed this duty to Plaintiffs and the other Class members because Plaintiffs and the other Class members compose a well-defined, foreseeable, and probable class of individuals whom Defendant should have been aware could be injured by Defendant's inadequate security protocols. Defendant actively solicited clients who entrusted Defendant with Plaintiffs' and the other Class members' PII/PHI when obtaining and using IT services and products. To facilitate these services, Defendant used, handled, gathered, and stored the PII/PHI of Plaintiffs and the other Class members. Attendant to Defendant's solicitation, use and storage, Defendant knew of its inadequate and unreasonable security practices with regard to their computer/server systems and also knew that hackers and thieves routinely attempt to access, steal and misuse the PII/PHI that Defendant actively solicited from clients who entrusted Defendant with Plaintiffs and the other Class members data. As such, Defendant knew a breach of its systems would cause damage to its clients and Plaintiffs and the other Class members. Thus, Defendant had a duty to act reasonably in protecting the PII/PHI of their clients.

64. Defendant also owed a duty to timely and accurately disclose to its clients and Plaintiffs and the other Class members the scope, nature, and

occurrence of the Data Breach. This disclosure is necessary so Plaintiffs and the other Class members can take appropriate measures to avoid unauthorized use of their PII/PHI, accounts, cancel and/or change usernames and passwords on compromised accounts, monitor their accounts to prevent fraudulent activity, contact their financial institutions about compromise or possible compromise, obtain credit monitoring services, and/or take other steps in an effort to mitigate the harm caused by the Data Breach and Defendant's unreasonable misconduct.

65. Defendant breached its duty to Plaintiffs and the other Class members by failing to implement and maintain security controls that were capable of adequately protecting the PII/PHI of Plaintiffs and the other Class members.

66. Defendant also breached its duty to timely and accurately disclose to the clients, Plaintiffs and the other Class members that their PII/PHI had been or was reasonably believed to have been improperly accessed or stolen.

67. Defendant's negligence in failing to exercise reasonable care in protecting the PII/PHI of Plaintiffs and the other Class members is further evinced by Defendant's failure to comply with legal obligations and industry standards, and the delay between the date of the Data Breach and the time when the Data Breach was disclosed.

68. The injuries to Plaintiffs and the other Class members were reasonably foreseeable to Defendant because laws and statutes, and industry

standards require Defendant to safeguard and protect its computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiffs' and the other Class members' PII/PHI.

69. The injuries to Plaintiffs and the other Class members also were reasonably foreseeable because Defendant knew or should have known that systems used for safeguarding PII/PHI were inadequately secured and exposed consumer PII/PHI to being breached, accessed, and stolen by hackers and unauthorized third parties. As such, Defendant's own misconduct created a foreseeable risk of harm to Plaintiffs and the other Class members.

70. Defendant's failure to take reasonable steps to protect the PII/PHI of Plaintiffs and the other members of the Class was a proximate cause of their injuries because it directly allowed thieves easy access to Plaintiffs' and the other Class members' PII/PHI. This ease of access allowed thieves to steal PII/PHI of Plaintiffs and the other members of the Class, which could lead to dissemination in black markets.

71. As a direct proximate result of Defendant's conduct, Plaintiffs and the other Class members have suffered theft of their PII/PHI. Defendant allowed thieves access to Class members' PII/PHI, thereby decreasing the security of Class members' financial and health accounts, making Class members' identities less secure and reliable, and subjecting Class members to the imminent threat of

identity theft. Not only will Plaintiffs and the other members of the Class have to incur time and money to re-secure their bank accounts and identities, but they will also have to protect against identity theft for years to come.

72. Defendant's conduct warrants moral blame because Defendant actively solicited its services to its clients, wherein it used, handled and stored the PII/PHI of Plaintiffs and the other Class members without disclosing that its security was inadequate and unable to protect the PII/PHI of Plaintiffs and the other Class members. Holding Defendant accountable for its negligence will further the policies embodied in such law by incentivizing larger IT service providers to properly secure sensitive consumer information and protect the consumers who rely on these companies every day.

SECOND CAUSE OF ACTION
Violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150
(On Behalf of the Plaintiffs and the California Subclass)

73. Plaintiffs incorporate by reference all previous allegations as though fully set forth herein.

74. Defendant violated section 1798.150(a) of the California Consumer Privacy Act by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII/PHI of Plaintiffs and the Class. As a direct and proximate result, Plaintiffs and the

Class's PII/PHI was subject to unauthorized access and exfiltration, theft, or disclosure.

75. Defendant is a business organized for the profit or financial benefit of is owners, and, on information and belief, buys, receives, sells, or shares for commercial purposes the PII/PHI of more than 50,000 consumers (of its clients). As a direct and proximate result of Defendant's acts, Plaintiffs and Class members were injured and lost money, property, and/or the interest in the confidentiality and privacy of their PII/PHI, and additional losses as described above.

76. Plaintiffs and Class members seek relief under California Civil Code section 1798.150(a), including but not limited to, recovery of actual damages; injunctive or declaratory relief; any other relief the court deems proper; and attorney's fees and costs.

77. Plaintiffs and the Class members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards customers' PII/PHI by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' PII/PHI, including Plaintiffs' and the Class members' PII/PHI. These individuals have an interest in ensuring that their PII/PHI is reasonably protected.

78. In addition to filing this Complaint, and on or about May 12 , 2021, Plaintiffs sent Defendant a notice letter to Defendant's registered service agent via

FedEx Priority Overnight as required by Civil Code section 1798.150(b). Assuming Defendant cannot cure the Data Breach within 30 days, and Plaintiffs believe any such cure is not possible under these facts and circumstances, then Plaintiffs intend to promptly amend this complaint to seek actual damages and statutory damages of no less than $100 and up to $750 per customer record subject to the Data Breach on behalf of the California Subclass as authorized by the CCPA.

THIRD CAUSE OF ACTION
Violation of the California's Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*.
(On Behalf of the Plaintiffs and the California Subclass)

79. Plaintiffs incorporate by reference all previous allegations as though fully set forth herein.

80. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq.* which prohibits unlawful, unfair, or fraudulent business acts or practices.

81. Defendant's conduct, as alleged above, is unlawful because it violates the Consumer Privacy Act of 2018, Civ. Code § 1798.100, et seq. (the "CCPA"), and other state data security laws.

82. Defendant stored the PII/PHI of Plaintiffs and the Class in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with

applicable regulations and that would have kept Plaintiffs' and all Class members' PII/PHI secure and prevented the loss or misuse of that PII/PHI.

83. Defendant failed to disclose to Plaintiffs and the Class that their PII/PHI was not secure. However, Plaintiffs and Class members were entitled to assume, and did assume, that their PII/PHI would be secured by Defendant. At no time were Plaintiffs and Class members on notice that their PII/PHI was not secure, which Defendant had a duty to disclose.

84. Defendant also violated California Civil Code § 1798.150 by failing to maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiffs' and the Class's PII/PHI.

85. If Defendant had complied with these legal requirements, Plaintiffs and all Class members would not have suffered the damages related to the Data Breach.

86. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes failing to adequately ensure the privacy, confidentiality, and security of PII/PHI entrusted to it, having unmonitored systems and programs, and failing to have basic data security measures in place.

87. Defendant also engaged in unfair business practices under the "tethering test." Defendant's actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

88. Instead, the PII/PHI of Plaintiffs and the Class were made accessible by Defendant to scammers, identity thieves, and other malicious actors, subjecting Plaintiffs and the Class to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violates the policies underlying the laws set out in the prior paragraph.

89. The harm caused by Defendant's unfair practices outweighs any potential benefits from those practices. Further, there were reasonable alternatives available to Defendant to further its legitimate business interests.

90. Plaintiffs and all Class members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In addition, Plaintiffs' and all Class members' PII/PHI was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value.

91. As a result of Defendant's violations of the UCL, Plaintiffs and members of the Class are entitled to restitution and other equitable relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly situated, respectfully requests that the Court enter an order:

a. Certifying the Class as requested herein;

b. Appointing Plaintiffs as Class Representative and undersigned counsel as Class Counsel;

c. Finding that Defendant engaged in the unlawful conduct as alleged herein;

d. Enjoining Defendant's conduct and requiring Defendant to implement proper data security practices, specifically:

    i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the PII/PHI of Plaintiffs and the Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and the Class members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiffs' and the Class members' PII/PHI;

v. prohibiting Defendant from maintaining Plaintiffs' and the Class members' PII/PHI on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems

on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII/PHI, as well as protecting the PII/PHI of Plaintiffs and the Class members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII/PHI;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers;

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

xviii. requiring Defendant to design, maintain, and test its computer systems to ensure that PII/PHI in its possession is adequately secured and protected;

xix. requiring Defendant to disclose any future data breaches in a timely and accurate manner;

xx. requiring Defendant to implement multi-factor authentication requirements;

xxi. requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; and

xxii. requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class members.

e. Awarding Plaintiffs and Class members damages;

f. Awarding Plaintiffs and Class members pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiff Meier, on behalf of her minor child G.C-M., and Plaintiff Doe, on behalf of themselves and the Class, demand a trial by jury on all issues so triable.

Respectfully Submitted

Dated: May 13, 2021

/s/Kate M. Baxter-Kauf

Karen Hanson Riebel (MN # 0219770)
Kate M. Baxter-Kauf (MN # 392037)
Maureen Kane Berg (MN # 033344X)
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Ave. South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com
mkberg@locklaw.com

Gayle M. Blatt, *Pro Hac Vice forthcoming*
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232
gmb@cglaw.com

Attorneys for Plaintiff and the Class